Cloud & Service Desk Support

Service Definition Document

IM-Client Confidential

2025

Contents

Introduction

This Service Definition describes the outsourced IT Support Service Desk provided by Managed 247. The service is aligned to the ITIL v4 framework, covering the key ITSM disciplines of Incident, Service Request, Problem, and Change Management.

The Service Desk supports both end-users and client IT teams, ensuring efficient issue resolution, enhanced governance, and predictable service outcomes.

This document defines the scope, operation, service levels, responsibilities, and acceptable use terms, ensuring there are no unknowns from service activation (onboarding) through to go-live and ongoing delivery.

The Service Desk Common Service Description is to be read alongside any of the related Service Definitions for the Managed 247 available tiered services:

Service Desk Delivery Options:

- Shared IT Desk
- Dedicated IT Desk
- Co-Managed IT Desk Services
- Dedicated OOH Service

Modular Capability Options:

- Level 1 – Frontline
- Level 2 – Technical Support
- Level 3 – Subject Matter Expert

ITIL Service Enhancements (ITIL As a Service):

- Availability Management
- Capacity Management
- Demand Management
- IT Service Continuity Management

This Common Service Definition explains the baseline standards, processes, and governance framework that apply to all Managed 247 Service Desk services. It should be read alongside the relevant Sub-Service Definition (e.g., Level 1, Shared, or Out-of-Hours Service Desk), which sets out the specific inclusions, exclusions, and commercial model. Together, they provide the full scope of the Managed 247 Service Desk offering.

How to Read This Document

This Common Service Definition sets the framework for all Managed 247 Service Desk offerings. It explains the standards, ITIL-aligned processes, available service levels, roles, and governance model that apply across every Service Desk engagement.

Who should read this document?

This document is intended for clients who wish to understand the baseline scope and governance of the Managed 247 Service Desk. It is most relevant to IT leadership, procurement, and service owners who need clarity on how the Service Desk operates.

How this document is structured

- ITIL Service Process Descriptions – defines how incidents, requests, problems, changes, and supporting ITSM processes are managed.
- Service Desk Tiers – outlines the three levels of support (L1, L2, L3) as independent building blocks.
- Service Operation – explains coverage options, support channels, onboarding, SLAs, reporting, and billing.
- Roles & Responsibilities – provides example RACIs to clarify accountability across MSP, client, and vendors.
- Relationship to Sub-Service Definitions.

This Common Service Definition is always read alongside a specific Service Definition for the chosen service option (e.g., Level 1 Service Desk Support, Shared Service Desk, Out-of-Hours Service Desk).

- The Common Service Definition sets the baseline standards.
- The Sub-Service Definition sets the specific inclusions, exclusions, and commercial model for that service.

How to use this document

Start with this Common Service Definition to understand the governance and operating model.

- Then refer to the sub-service definition that applies to your chosen service option to see the specific scope and pricing model.
- Together, these documents provide a full picture of what is included in the Managed 247 Service Desk.

ITIL Service Process Descriptions

Incident Management

Purpose

Restore normal service operation as quickly as possible when an IT service is disrupted, minimising business impact.

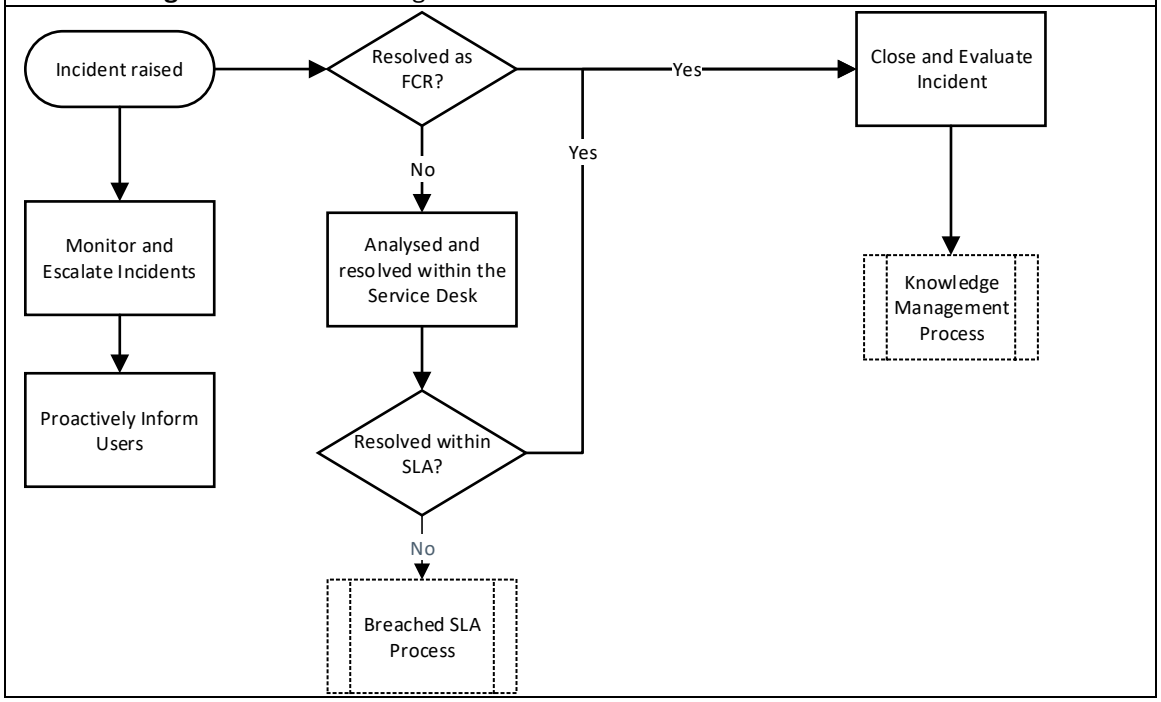
Approach

- All incidents logged via Service Desk (phone for urgent, or portal/email for all others).
- Categorisation agreed with client during transition for reporting and SLA alignment.
- Prioritised based on Impact and Urgency.

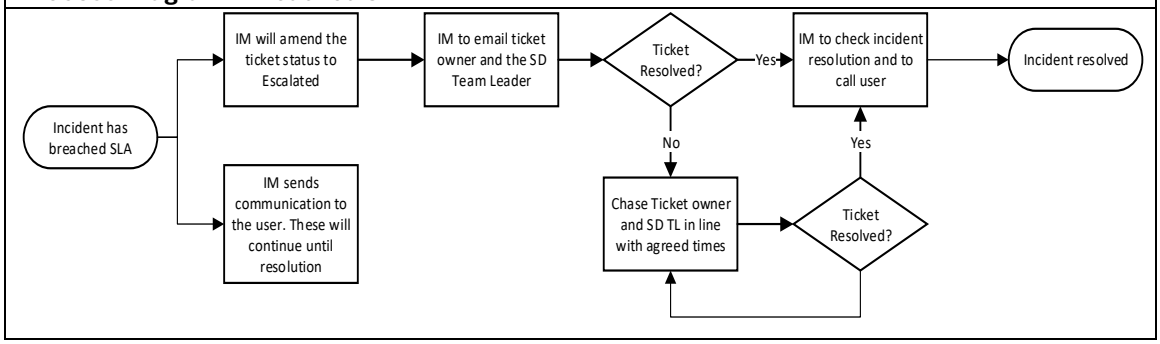
Process Overview

1. Log Ticket
    - Incidents logged via phone, email, chat, or portal into the Service Desk system.
2. Immediate Resolution (First Call Resolution – FCR)
    - If possible, resolved at first contact using knowledge base or scripts.
3. Progress & Escalate
    - If unresolved, assigned to Level 2/3, Client Resolver, or Vendor.
4. Investigate & Resolve
    - Technical teams analyse and resolve; workarounds applied if needed.
5. Monitor & Manage SLA
    - Incident Manager monitors progress; breaches escalated.
6. User Communication
    - Users proactively updated if service disruption impacts them.
7. Close Incident
    - Resolution validated with user; incident formally closed.
8. Problem Management Linkage
    - Recurring or major incidents reviewed for root cause.
9. Reporting & Knowledge Update
    - Incidents included in daily/weekly/monthly reporting.
    - Fixes/workarounds added to knowledge base.

Process Diagram – Incident Management



Process Diagram – Breached SLA



Incident Management – Example RACI

Activity	MSP L1	MSP L2	MSP L3	Client Resolver Group	Vendor
Log & Categorise Incident	R	–	–	–	–
Initial Diagnosis & Resolution	R	–	–	–	–
Escalation	A	R	R	R (if in-scope)	R (if in-scope)
Resolution & Recovery	R	R	R	R	R
Closure Confirmation	R	–	–	–	–

Additional Considerations

- P1 incidents can only be raised by authorised users via phone.
- DR/BCP scenarios are excluded and handled under Continuity Management.
- Escalation can be functional (resolver groups) or hierarchical (management).

Event Management

Purpose

Detect, analyse, and respond to events in IT systems to maintain normal operations and prevent incidents.

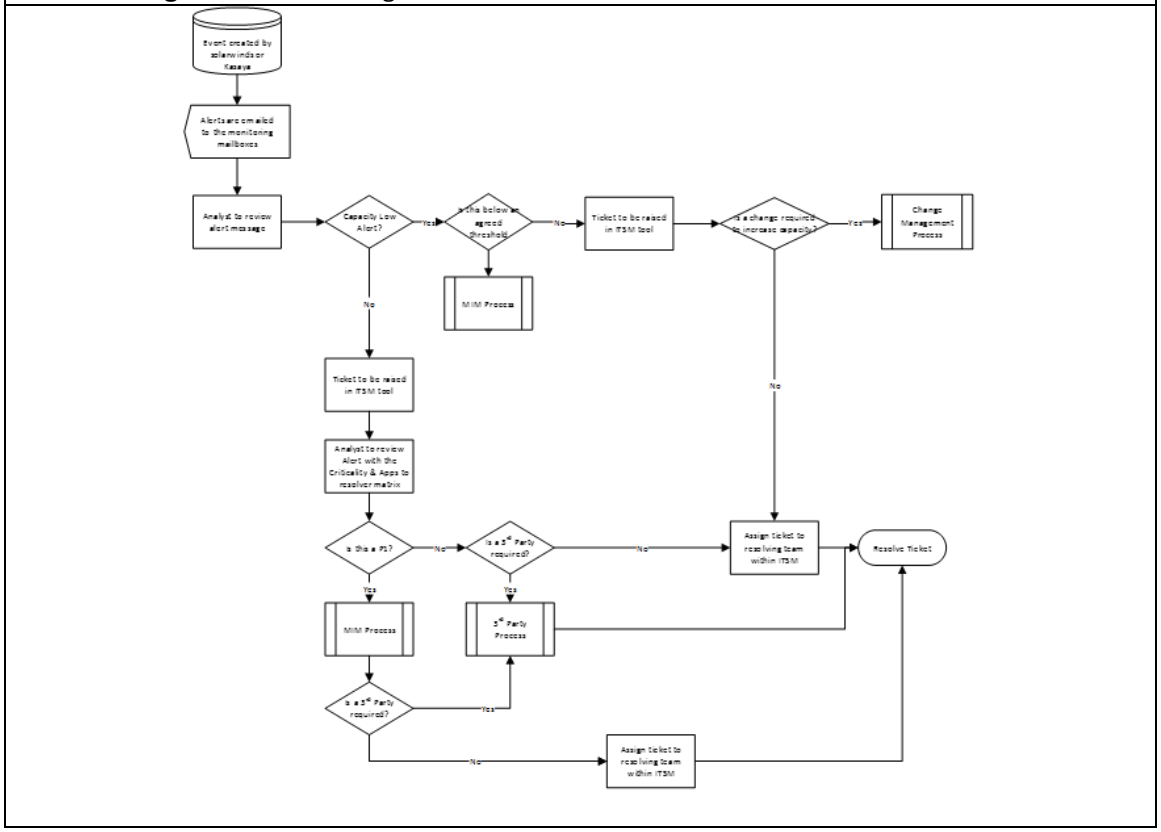
Approach

- Managed 247 monitors systems via Observability, Remote Management Monitoring and Network Performance Monitoring solutions
- Events categorised as informational, warning, or exception.
- Supports proactive response to potential issues.

Process Overview

1. Detect event (monitoring platform).
2. Categorise event (info, warning, exception).
3. Log event if action required.
4. Escalate to Incident Management where necessary.
5. Track and close.

Process Diagram – Event Management



Event Management – Example RACI

Activity	**MSP L1**	**MSP L2**	**MSP L3**	**Client Resolver**	**Vendor**
Monitor Systems & Capture Events	R	–	–	–	–
Filter & Correlate Events	R	R	–	–	–
Classify Event (Informational, Warning, Exception)	R	R	–	–	–
Escalate Exception Events to Incident Mgmt	A	R	R	R (if in-scope)	R (if in-scope)
Analyse Root Cause for Repeated Events	–	R	A	R (if infra/app owned)	R
Implement Event-driven Automation/Remediation	R	R	A	–	–
Update Knowledge Base with Event Patterns	R	R	A	–	–
Report on Event Trends & Service Impact	A	R	R	–	–

Additional Considerations

- Capacity-related events are managed in line with Capacity Management.
- Event correlation tools reduce noise and highlight meaningful alerts.

Service Request Fulfilment

Purpose

Provide a consistent process for handling day-to-day user requests (e.g., password resets, software installs, access).

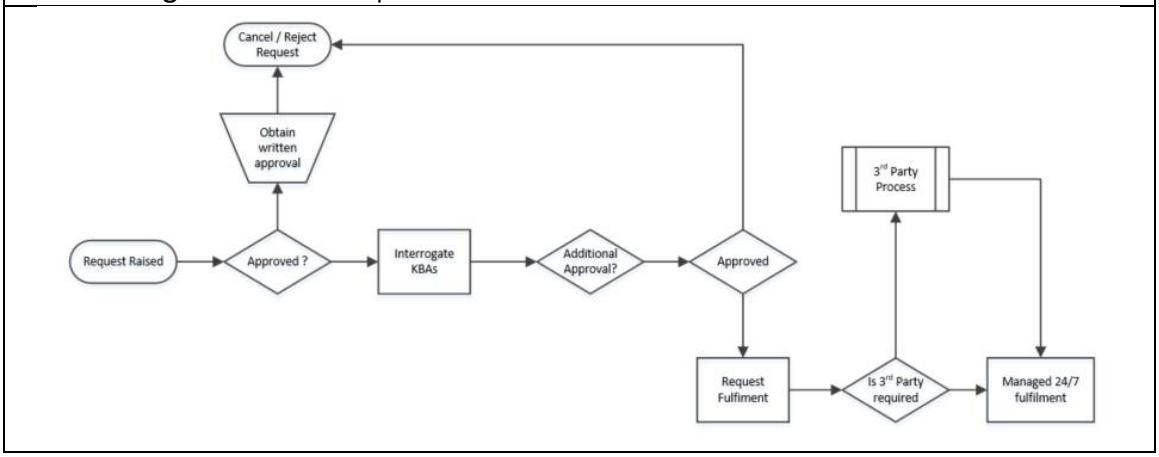
Approach

- Requests submitted via Service Desk.
- Authorised against Service Catalogue (client's or one built during transition).
- Managed through standardised fulfilment models.

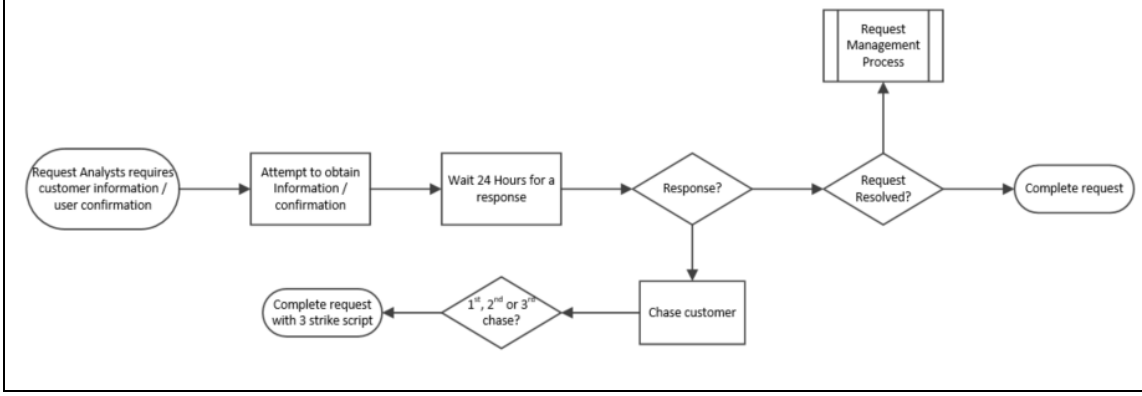
Process Overview

1. Log service request.
2. Verify authorisation.
3. Fulfil request via predefined model.
4. Notify user of completion.
5. Close request.

Process Diagram – Service Request Fulfilment



Process Diagram – Three Strike Process



Service Request Management – Example RACI

Activity	MSP L1	MSP L2	MSP L3	Client Resolver Group	Client Approver
Receive & Log Request	R	–	–	–	–
Validate Authorisation	R	–	–	–	A
Fulfil Request	R	R	R (if complex)	R (if in-scope)	–
Confirm Completion	R	–	–	–	–

Additional Considerations

- Unauthorised requests returned or escalated for approval.
- Catalogue integration improves speed and transparency.

Problem Management

Purpose

Identify and remove the root cause of recurring incidents to prevent future disruption.

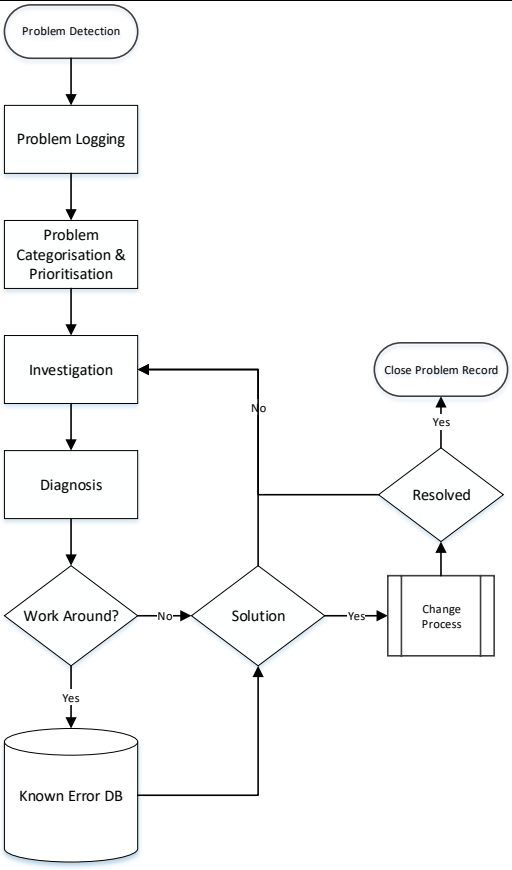
Approach

- Incidents are linked to underlying Problems.
- RCA performed for major or recurring issues.
- Solutions or workarounds documented and shared.

Process Overview

1. Log problem from linked incidents.
2. Categorise and prioritise.
3. Investigate and perform RCA.
4. Document solution or workaround.
5. Review and validate.
6. Close problem record.

Process Diagram – Problem Management



Problem Management – Example RACI

Activity	MSP L1	MSP L2	MSP L3	Client Resolver Group	Vendor
Detect & Log Problem	R	R	–	–	–
Root Cause Analysis	–	R	A	R (if infra/app owned)	R
Workaround Definition	R	R	A	–	–
Permanent Fix	–	R	A	R (if in-scope)	R
Problem Closure	–	R	A	–	–

Additional Considerations

- Major Problems trigger formal reviews.
- Problem records feed into Knowledge Management.
- DR/BCP exclusions apply.

Change Management

Purpose

Change Management ensures that any updates, alterations, or additions to a Client's IT services are carried out in a controlled, timely, and safe manner, delivering business benefit while minimising the risk of disruption.

Approach

- As part of the Managed Service, Managed 247 will work to adopt and align with the Client's existing Change Management processes, unless Managed are the Change Owner, where Managed will provide full Change Management.
- During Service Transition and Activation, Managed 247 will:
    - Review Client's existing processes.
    - Agree how change requests will be submitted and authorised (by end-users, Managed 247, or both).
    - Define required approval levels and timescales.

If the Client does not have a formal ITIL-aligned Change Management process, Managed 247 will:

- Agree during transition whether a separate project should be initiated to establish or improve this process.

If the Client does have an ITIL-aligned process, Managed 247 will:

- Review and incorporate it into the service delivery model.
- Manage Emergency, Normal, and Standard changes according to ITIL best practice.
- Adopt Client's documented change models where appropriate for a co-sourced environment.

Types of Requests for Change (RFC)

- **Project**
  These types of RFCs are pre-approved and will be raised for the purpose of the Projects that full under the scope of Change Management. These are for awareness purposes only.
- **Standard**
  These types of RFCs are pre-approved by the customer & technical towers, where a standard template exists with pre-defined implementation steps where the risks are known upfront. These types of RFCs still need to be raised prior to the work being carried out for visibility purposes and awareness.
- **Normal**
  These types of RFCs do not have pre-defined implementation plans and the risks and impact are unknown and will require CAB approval.
- **Emergency**
  These types of RFCs should be raised as part of a solution to resolve an ongoing P1 incident or to stop a potential P1 incident occurring where an unexpected error or threat has occurred or where they are required to be made immediately. The detail of the RFC must be to the same standard as the Normal RFCs.

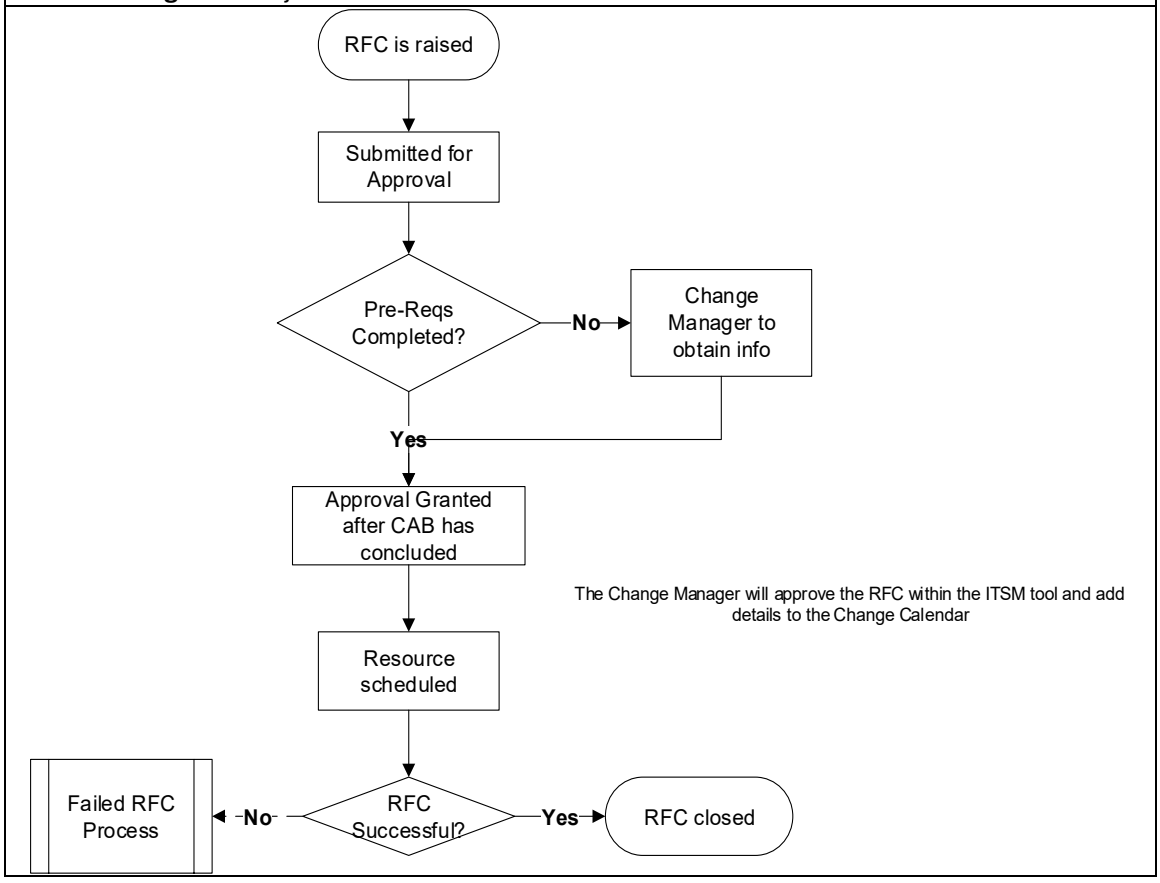
Process Overview

All changes to Configuration Items (CIs) must go through the agreed change process. Managed 247 and Client will share CI Administrator access, but no direct changes will be made outside the agreed framework.

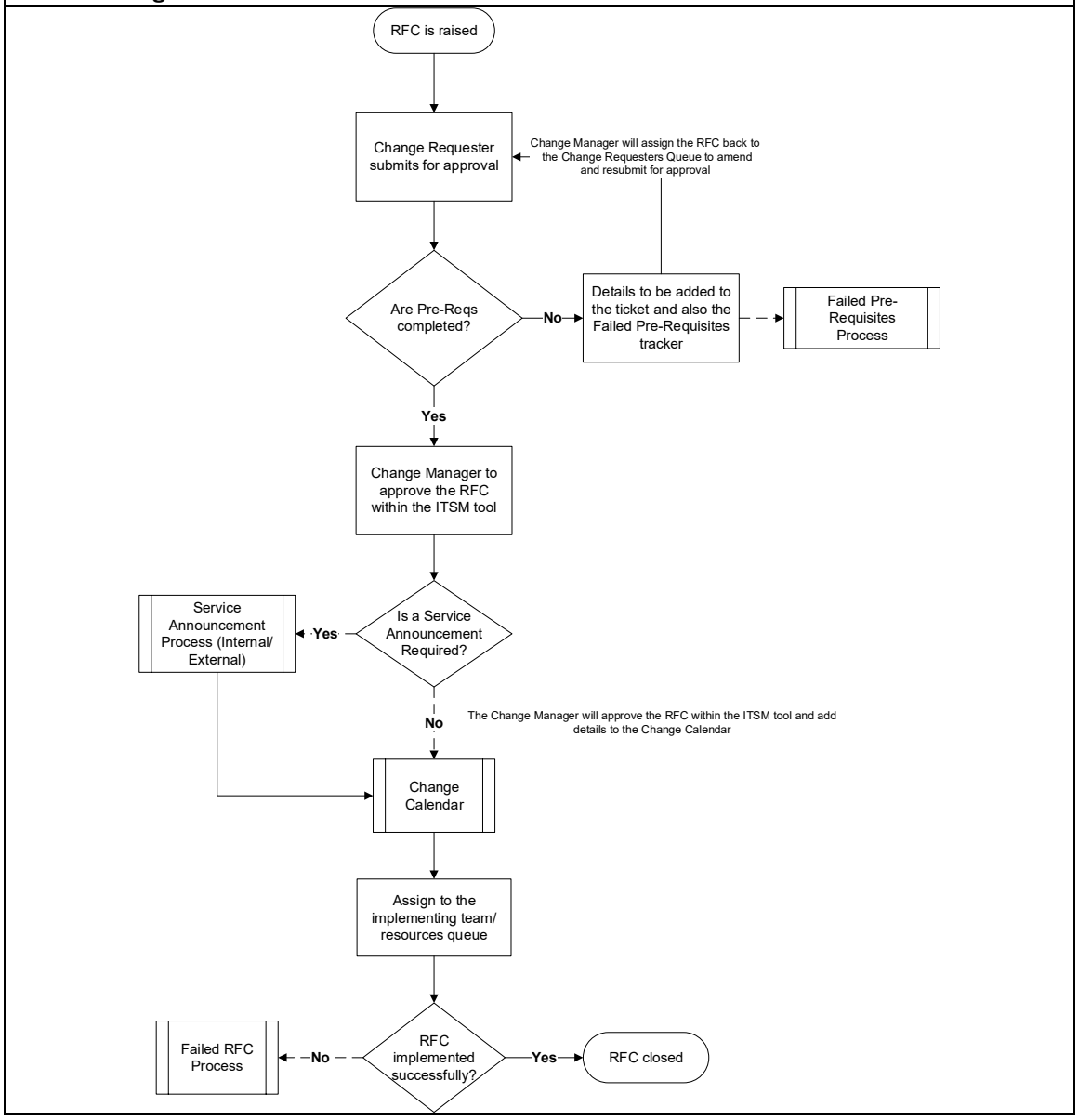
The Managed 247 Change Process follows ITIL best practices:

1. Receive & Record Request for Change (RFC) – capture details of the proposed change.
2. Initial Review – confirm appropriateness before formal evaluation.
3. Change Evaluation – assess technical impact, business benefit, and risks.
4. Authorisation – obtain the required approvals (methods can include email, portal, or verbal if pre-agreed).
5. Build & Test – prepare and validate changes in a controlled environment where appropriate.
6. Authorise Deployment – confirm readiness for implementation.
7. Deployment – execute the change in a controlled manner.
8. Review & Verify – confirm the change is successful and that no issues remain.
9. Close Change – formally complete the change in the system.

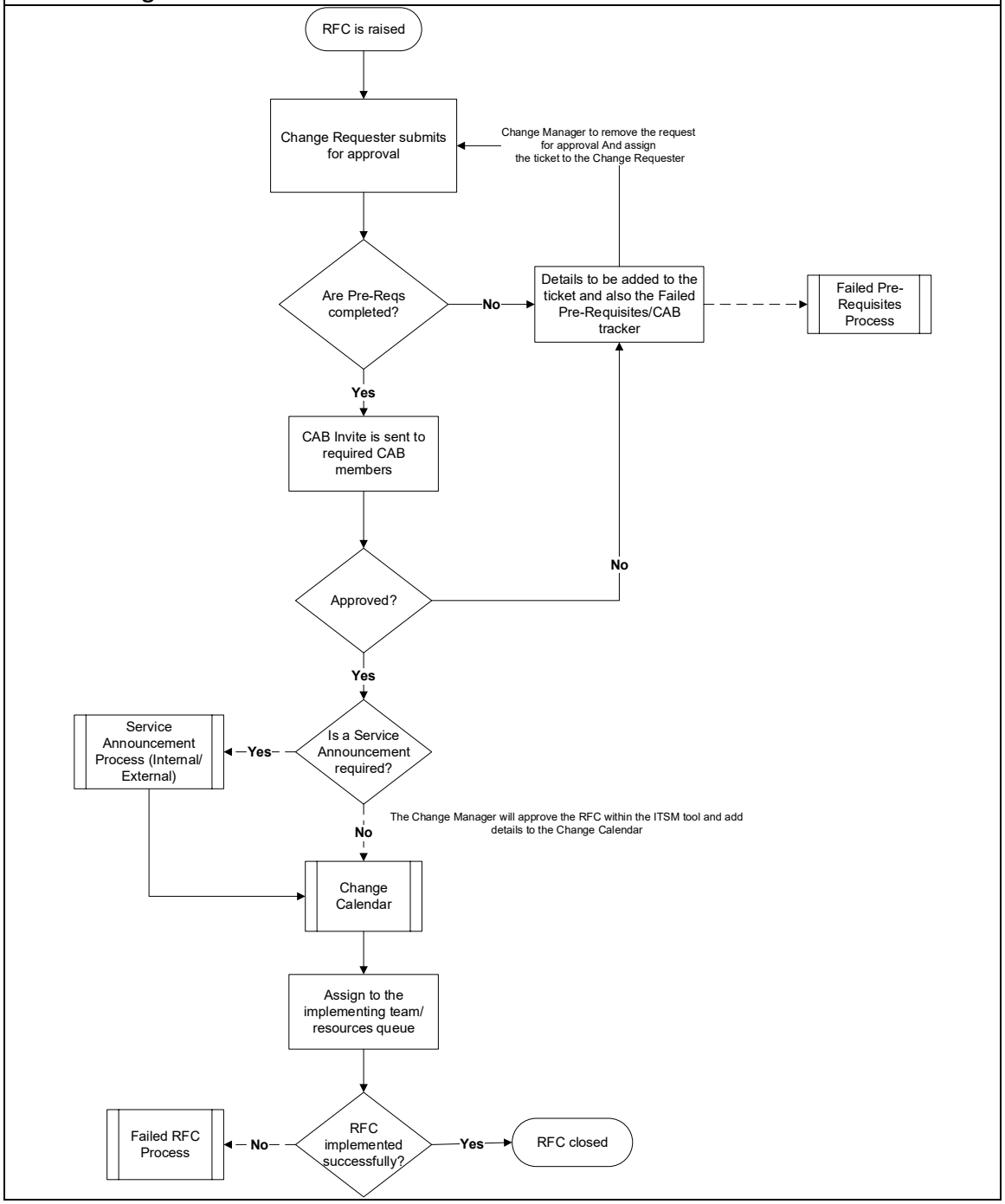
Process Diagram - Project RFC



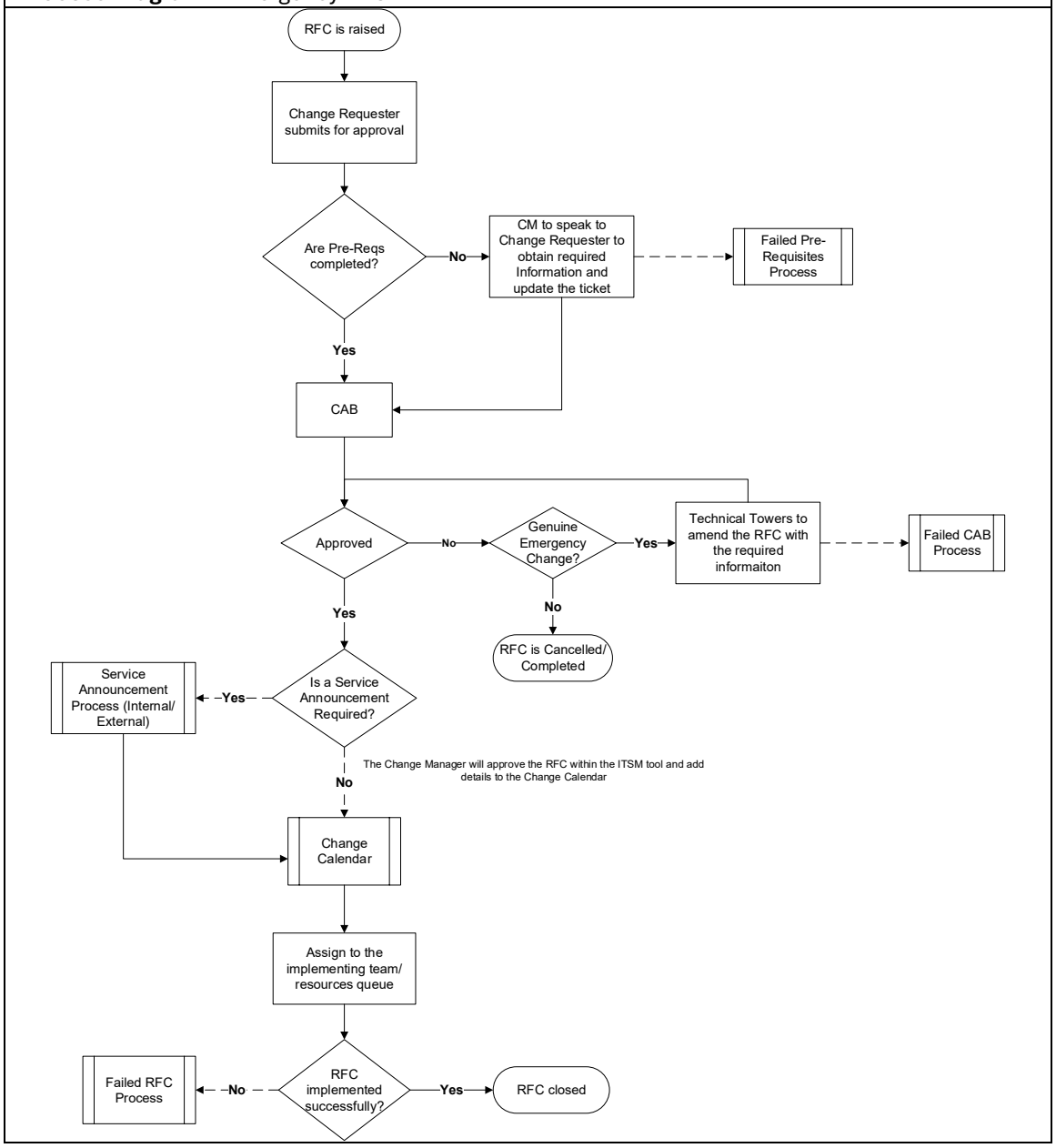
Process Diagram - Standard RFC



Process Diagram - Normal RFC



Process Diagram - Emergency RFC



Problem Management – Example RACI

Activity	**MSP L1**	**MSP L2**	**MSP L3**	**Client Resolver Group**	**Vendor**
Detect & Log Problem	R	R	–	–	–
Root Cause Analysis	–	R	A	R (if infra/app owned)	R
Workaround Definition	R	R	A	–	–
Permanent Fix	–	R	A	R (if in-scope)	R
Problem Closure	–	R	A	–	–

Additional Considerations

- SLAs: Suggested SLAs for Change Priorities (Emergency, Normal, Standard) are defined in the Service Level section.
- Post-Implementation Review: Required for all Major Changes to ensure learning and improvement.
- Install, Move, Add, Change (IMAC): Client must notify Managed 247 in writing of any planned IMAC activities to Managed Elements. If the Client lacks the capability, Managed 247 can provide IMAC support.
- Change Advisory Board (CAB) Scheduling: CAB will be held daily at 15:00. Daily Cut off for Normal RFCs to be submitted to CAB for approval is 14:00 and between 14:00 & 15:30 there will be a change freeze where no RFC approvals are requested, however, they can still be created and saved. Where possible any Normal RFCs should be raised for the CAB the day before it is required to be implemented at the latest. However, there will be times for justified reasons why an RFC will need to be raised on the day that it is to be implemented.

Knowledge Management

Purpose

Ensure solutions, fixes, and workarounds are captured and shared to improve resolution times.

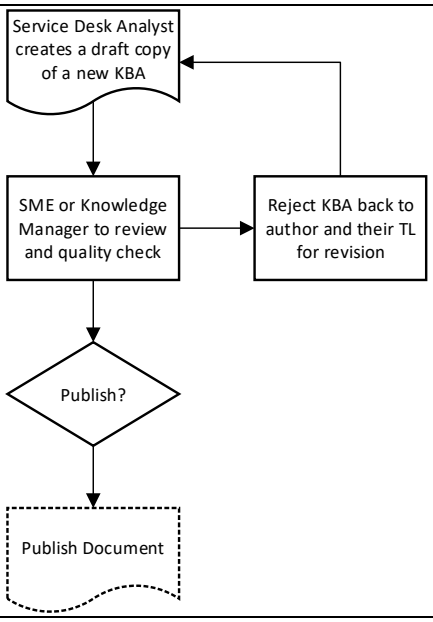
Approach

- Knowledge captured during Incident and Problem Management.
- Published in central Knowledge Base.
- Available to Service Desk and, where appropriate, end-users.

Process Overview

1. Identify new knowledge (from incident/problem resolution).
2. Create article and validate accuracy.
3. Publish to knowledge base.
4. Use knowledge in future ticket resolution.
5. Update and retire articles as needed.

Process Diagram – Creating New KB Article



Knowledge Management – Example RACI

Activity	MSP L1	MSP L2	MSP L3	Client Resolver	Vendor
Identify Knowledge Article Candidates (from Incidents/Requests)	R	R	R	C	C
Draft Knowledge Article	R	R	A	C	C
Review & Approve Knowledge Article	–	A	A	C	–
Publish to Knowledge Base	R	A	A	–	–
Use Knowledge for Ticket Resolution	R	R	R	–	–
Maintain & Update Articles	R	A	A	C	C
Retire Obsolete Articles	–	R	A	–	–
Report on Knowledge Usage & Effectiveness	A	R	R	–	–

Additional Considerations

- Knowledge reduces repeat workload on Service Desk.
- Knowledge Base continuously updated as part of continual service improvement.

Vendor Escalation Management

Purpose

Ensure timely and effective escalation to third-party vendors for complex incidents or service requests that cannot be resolved at Level 1 or Level 2. Vendor Escalation provides access to specialist expertise while ensuring the client remains informed and resolution progress is managed.

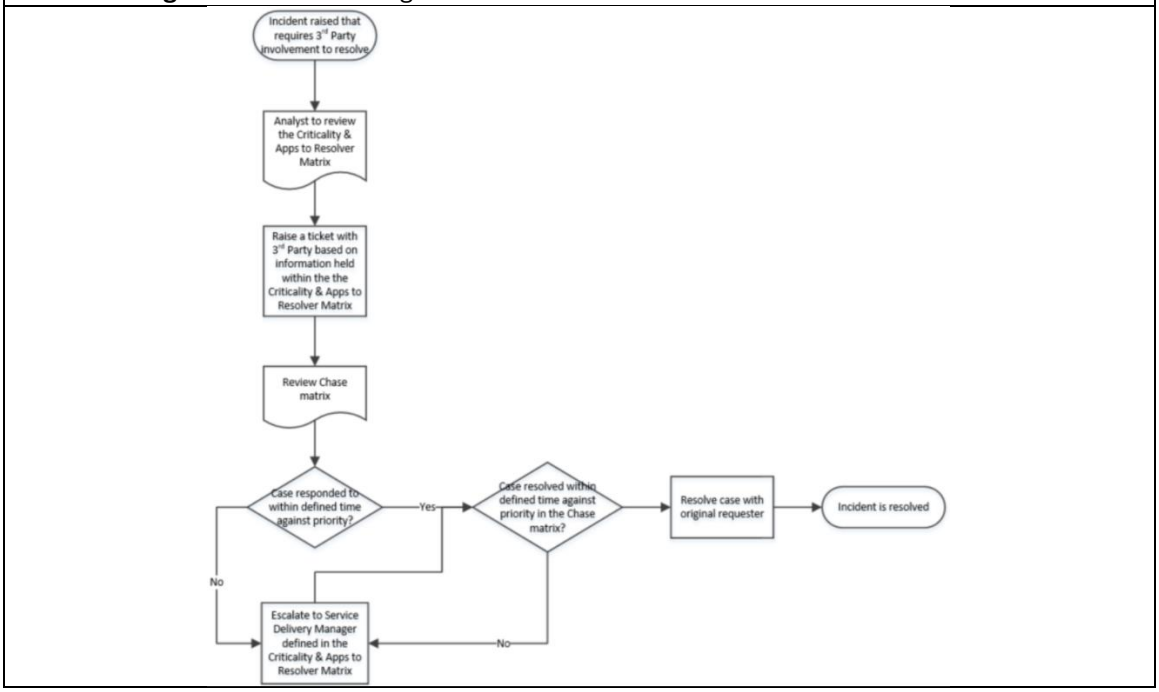
Approach

- Applicable only at Level 3 where specialist or vendor support is required.
- Managed 247 coordinates directly with the vendor, acting as the escalation point.
- Vendor contracts and points of contact are identified during Service Transition.
- Where Managed 247 holds the vendor contract, full escalation ownership is retained by Managed 247.
- Where the client holds the vendor contract, Managed 247 coordinates on the client's behalf and tracks progress through to resolution.
- Focus is on resolution of the escalated issue, not vendor performance management or contract governance.

Process Overview

1. Identify Vendor & Escalation Path – Confirm contract holder, escalation procedure, and contact details.
2. Engage Vendor – Raise and track ticket with vendor support team.
3. Coordinate Investigation – Provide required diagnostic information, logs, or evidence.
4. Track Resolution – Monitor progress and chase vendor updates against the vendor's SLA/OLA.
5. Communicate Updates – Keep the client informed throughout the escalation.
6. Validate Fix & Close – Confirm resolution, validate testing, and update knowledge base if applicable.

Process Diagram – Vendor Management



Vendor Management – Example RACI

Activity	MSP	Client	Vendor	Client Service Owner
Identify Vendor & Escalation Path	R	A	C	I
Raise Escalation (MSP-held contract)	R / A	I	R	I
Raise Escalation (Client-held contract)	C	R / A	R	I
Provide Diagnostic Info & Evidence	R	C	C	I
Track & Monitor Progress	R	C	A	I
Communicate Updates	R	I	C	I
Validate Fix & Close Ticket	R	C	C	I
Update Knowledge Base (if applicable)	R	C	C	I

Additional Considerations

- This process does not include vendor performance management or contract negotiation — it is strictly escalation for issue resolution.
- Escalations are logged in the Service Desk system for tracking and reporting.
- Vendor escalation activities are included in incident and problem reports for transparency.
- Responsibility for overall vendor contract governance remains with the client (unless otherwise contracted separately).

Service Desk Tiers

The Service Desk tiers are offered as independent service blocks. Each level can be consumed individually or combined, depending on client requirements. This flexible model allows clients to outsource selected capabilities (e.g., only Level 3 SME escalation) or take the full end-to-end Service Desk. The same tiered structure underpins all aligned services, including Shared IT Desk, Dedicated IT Desk, Co-Managed Services, Out-of-Hours, ITIL-as-a-Service, and ServiceNow ITSM Service, ensuring consistency, scalability, and integration across delivery models.

Service Desk Tiers Comparison

The following table summarises the inclusions and scope of each Service Desk tier. This side-by-side view provides a comparison of the tiers at a glance.

Feature / Scope	**Level 1 – Frontline / Triage**	**Level 2 – Technical Support**	**Level 3 – Specialist / Vendor**
Purpose	First point of contact, resolve common user issues quickly.	Provide deeper technical troubleshooting for infra/app issues.	Expert-level support and vendor engagement for complex issues.
Examples	Password resets, account unlocks, basic software queries, printer issues.	Server performance issues, application errors, network faults, software deployment.	Critical DB outage, security incidents, complex infra faults, RCA for recurring issues.
Scope	Ticket logging, categorisation, prioritisation, first-line fix.	Advanced diagnostics, configuration, standard changes.	Specialist troubleshooting, vendor liaison, RCA, advisory input.
Escalation	Escalates unresolved issues to L2 or L3.	Escalates unresolved issues to L3 or vendor if required.	Engages vendors (Managed 247 or client-held contracts).
Knowledge & Problem Mgmt	Uses knowledge base/runbooks to resolve common issues.	Updates knowledge base; identifies patterns for Problem Mgmt.	Provides RCA; feeds improvements into Problem & Change Mgmt.
Additional Considerations	High first-call resolution target; improves user satisfaction.	Bridges end-user issues and specialist/vendor support.	Standalone option; supports governance, CAB, and continual service improvement.

The primary differentiators across sub-services are coverage model (shared, dedicated, co-managed), scope of responsibility (L1–L3), and service hours (standard vs out-of-hours). These are defined in the aligned sub-service definitions.

Level 1 – Frontline / Triage

Function Key Capabilities

- First point of contact for all users.
- Logging via phone, email, chat, or portal.
- Initial troubleshooting (password resets, account unlocks, BAU issues).
- Incident classification (P1–P4) and routing.
- High first-call resolution and first-time fix focus.

Purpose

Provide the first point of contact for end-users and IT staff, logging and resolving common issues quickly to minimise disruption.

Approach

- Focus on fast resolution of high-volume, low-complexity issues.
- Use knowledge articles, scripts, and runbooks for consistency.
- Escalate issues that cannot be resolved at first contact.

Process Overview

1. User contacts Service Desk via phone, email, chat, or portal.
2. Ticket logged, categorised, and prioritised (P1–P4).
3. First-line troubleshooting applied.
4. Issue resolved or escalated to Level 2/3 or client resolver group.
5. Ticket closed with user confirmation.

Examples

- Password resets and account unlocks.
- Software usage queries (e.g., MS Office).
- Printer or peripheral connectivity.
- Logging incidents or service requests for escalation.

Additional Considerations

- Drives high first-call resolution rate.
- Reduces ticket backlog by resolving simple issues immediately.
- Provides visibility into demand patterns through categorisation.

Level 2 – Technical Support

Function Key Capabilities

- Escalation point from Level 1.
- Technical troubleshooting for infrastructure and application issues.
- Standard service requests requiring configuration.
- Advanced diagnostics (remote access, log analysis).
- Identifies patterns for Problem Management.

Purpose

Provide deeper technical support for incidents and service requests that cannot be resolved at Level 1.

Approach

- Handle infrastructure and application-related issues.
- Apply advanced diagnostics, tools, and configuration knowledge.
- Identify patterns for Problem Management and feed into Change.

Process Overview

1. Ticket escalated from Level 1 or raised directly.
2. Technical troubleshooting (infrastructure, apps, endpoints).
3. Implement standard changes and service requests requiring configuration.
4. Validate fix with user or IT team.
5. Update knowledge base if applicable.
6. Close ticket.

Examples

- Server performance troubleshooting.
- Application configuration issues.
- Network connectivity failures.
- Deploying software via remote management tools.

Additional Considerations

- Provides bridge between end-user issues and specialist/vendor support.
- Supports standard changes under agreed models.
- Works closely with Problem Management to identify recurring issues.

Level 3 – Specialist / Vendor Escalation

Function Key Capabilities

- Handles complex incidents and recurring issues.
- Vendor engagement (Microsoft, OEMs, specialist applications).
- Provides RCA and problem remediation.
- Executes advanced changes with CAB oversight.
- SME advisory input for continuous improvement.

Purpose

Deliver expert-level support for complex or critical issues, including vendor and SME engagement, to ensure end-to-end resolution.

Approach

- Apply specialist skills for advanced troubleshooting and RCA.
- Engage third-party vendors under Managed 247 or client-held support contracts.
- Provide advisory input into Problem and Change Management.

Process Overview

1. Ticket escalated from Level 2 or raised directly (SME-only contracts).
2. Deep technical investigation and root cause analysis.
3. Engage vendors where Managed 247 holds contracts, or coordinate with client vendors.
4. Implement solution or workaround.
5. Provide RCA and recommendations for service improvement.
6. Close ticket with documentation of fix.

Examples

- Critical database outage requiring vendor engagement.
- Security incident requiring SME intervention.
- Complex infrastructure faults (e.g., storage cluster failure).
- RCA for recurring application failures.

Additional Considerations

- Can be purchased standalone (e.g., outsources SME/vendor escalation).
- Supports vendor engagement depending on contract ownership.
- Provides advisory role for continual service improvement.
- Feeds into governance forums, CAB, and Problem Management.

Example Service Desk Level Workflows

- **Password Reset:** Resolved at L1.
- **Server Performance Issue**: L1 triages → L2 resolves.
- **Critical Database Outage:** L1 logs as P1 → L2 validates → L3 engages vendor & resolves.

Key

✓	Included
-	Not Included
•	Service Enhancement

Functionality / Feature	Level 1 (Frontline)	Level 2 (Technical)	Level 3 (Specialist)
Ticket Logging & Categorisation	✓	✓ (on escalation)	✓ (on escalation)
Password Resets / Basic BAU	✓	-	-
Incident Prioritisation (P1–P4)	✓	✓	✓
Service Request Fulfilment (JML included in standard)	✓ (standard)	✓ (technical)	✓ (advanced)
Technical Troubleshooting	-	✓	✓
Diagnostics & Log Analysis	-	✓	✓
Problem Trend Analysis	-	✓ (identify)	✓ (RCA & eliminate)
Change Execution	-	✓ (standard)	✓ (complex/major)
Vendor Management	-	Limited	•
Root Cause Analysis Reports	-	-	•
Service Delivery Management*	•	•	•

*. SDM is a separate service enhancement, a real-time self-service reporting portal is provided as standard.

Service Operation

Support Coverage Options

Managed 247 offers several coverage tiers so clients can select the level of availability that best matches their business needs. These tiers define the hours of operation, days covered, and whether public holidays are included. The four standard options are:

Business Hours

- 08:00–18:00, Monday to Friday (public holidays included).
- Best suited for organisations operating within UK business hours.

Extended Hours

- 08:00–20:00, Monday to Saturday (public holidays included).
- Ideal for businesses with extended working hours or Saturday trading.

24x7 Cover

- 24 hours a day, 7 days a week, 365 days a year (public holidays included).
- The most commonly selected tier, balancing cost with comprehensive coverage for critical services and global operations.

Dedicated Resolver Focus

- 24x7x365 with enhanced resolver engagement and dedicated escalation handling.
- Recommended for enterprise clients with complex infrastructure or those requiring maximum assurance and continuity.

Additional Options

- Support hours can be tailored (e.g., region-specific, split-shift cover).
- Out-of-Hours (OOH) support is available as a separate service definition but integrates seamlessly into the Service Desk model.

Support Coverage Options Matrix

The following matrix provides a side-by-side comparison of the standard support coverage tiers. This helps clients quickly identify which option aligns with their business requirements.

Feature / Coverage	(Business Hours)	(Extended Hours)	(24x7 Cover)	(Dedicated Resolver)
Hours of Operation	08:00–18:00	08:00–20:00	24x7x365	24x7x365
Days Covered	Mon–Fri	Mon–Sat	Every Day	Every Day
Public Holidays	Included	Included	Included	Included
Typical Use Case	Standard UK office hours	Extended hours / Saturday trading	Most common choice: cost + full coverage	Enterprise clients requiring dedicated response & resolver focus

Support Channels

Clients can contact the Service Desk through a variety of channels, ensuring accessibility and flexibility based on urgency and preference. Each channel is integrated into the ITSM platform, providing a consistent experience and full audit trail.

- **Phone** – Best for urgent issues (e.g., P1 incidents) requiring immediate attention.
- **Email** – Suitable for non-urgent issues or when attaching supporting information.
- **ITSM Web Portal** – Provides self-service logging, ticket tracking, and access to knowledge articles.

Support Channel Recommendation Matrix

The following matrix provides guidance on which support channel to use based on the type and urgency of the request. This helps ensure incidents and requests are directed to the most efficient route for resolution.

Request Type / Urgency	**Phone**	**Email**	**Web Portal**	**Chat (Halo only)**
P1 – Critical Incident (Service outage, urgent impact)	**Primary** – immediate response	**Backup only** – slower response	–	–
P2 – High Incident (Degraded service, multiple users affected)	**Preferred** for fast escalation	**Acceptable** if details required	–	–
P3 – Medium Incident (Single user, non-urgent impact)	–	**Suitable**	**Preferred** for tracking and self-service	**Quick** queries
P4 – Low / Service Request (BAU request, password reset, software install)	–	**Suitable**	**Preferred** – ensures request model applied	If available knowledge article / quick resolution

Service Pre-requisites

- User directory and contact access
- Resolver group details
- Agreed ticket baselines
- System/network access for troubleshooting
- Defined escalation paths

Onboarding & Transition

The onboarding process includes knowledge transfer, runbook creation, and service readiness. Early Life Support (ELS) runs for 90 days post go-live, ensuring stability and service adoption.

SLA's start after the initial 90 day ELS period, and service is live.

Service Termination

Formal offboarding process including knowledge handover, closure of open tickets, and final reporting. A chargeable service offboarding enhancement service is available upon request.

See exit strategy documents.

Service Levels & Performance Metrics

KPIs & Metrics

- Response Time (by priority)
- Resolution Time (by priority)
- Average Speed to Answer (ASA)
- Net Promoter Score (NPS)/Service Lifecycle/Quality Management

SLA Targets

Priority	Response Time	Resolution Target
P1 – Critical	15 min	4 hrs
P2 – High	30 min	8 hrs
P3 – Medium	2 hr	72 Hours
P4 – Low	12 hrs	120 Working Days

SLA Enforcement Options

Three SLA enforcement models are available:

1. Performance-Based SLA: SLAs tracked for governance and service improvement, no penalties.
2. Service Credit SLA: Financial/service time credits applied if SLA breaches exceed agreed thresholds.
3. Break-clause for extended period of missed SLA, executive escalation period. Assumes service going into hyper-care.

Acceptable Use Policy (Ticket Consumption)

The Service Desk operates on a ticket consumption model:

- All tickets (incidents, service requests, changes) consume equal units.
- Monthly ticket baseline allowance agreed per contract.
- “X”% agreed flex allowance before overage applies.
- End-user and IT team tickets consume allowance.
- Monitoring/system alerts are excluded unless MSP monitoring service is contracted.
- Persistent overage is raised in service delivery reporting or billed per ticket for overages.

Reporting & Analytics

Standard included Service

- Monthly dashboards (volumes, SLAs, KPIs)
- Quarterly service reviews (trend analysis, improvements)

Delivered by the Account Manager function, unless a Service Delivery Manager is aligned.

Service Delivery Management Enhancement

See the Service Delivery Management Service Definition for solution offering.

Roles & Responsibilities

To ensure clarity, Managed 247 and the Client will agree responsibilities across all ITIL processes during service transition. The below examples illustrate how roles are typically allocated across the Service Desk tiers, Client Resolver Groups, and Vendors. Specific allocations may vary based on the selected service model (Shared, Dedicated, Co-Managed, etc.) and will be finalised in the service contract (service executable).

Typical RACI Roles:

MSP Level 1 (Frontline / Triage)

First point of contact for all incidents and requests. Responsible for logging, categorisation, initial diagnosis, and resolving common user issues quickly.

MSP Level 2 (Technical Support)

Provides advanced troubleshooting for infrastructure and applications. Escalation from L1 and fulfils more complex service requests or standard changes.

MSP Level 3 (Specialist / Vendor Escalation)

Delivers expert-level support as subject matter experts, root cause analysis, and engages directly with third-party vendors where appropriate. Often handles complex or critical incidents.

Client Resolver Group

Internal client teams responsible for business applications, infrastructure, or services not in scope of the MSP contract. They act as a resolver when the issue sits outside MSP responsibility.

Vendor

Third-party suppliers or partners who provide manufacturer or application-specific expertise. The MSP coordinates with them where Managed 247 holds the contract, or works with the client to manage vendor escalations.

Cross-service Providers

Additional service provider teams responsible for specific outsource business applications, infrastructure, or services not in scope of the MSP contract. They act as a resolver when the issue sits outside MSP responsibility.

CAB (Change Advisory Board)

Formal governance body that reviews and authorises significant or high-risk changes. Ensures risks, impacts, and dependencies are considered before approval.

Client Service Owner

The client's accountable owner for IT service delivery. Informed of major activities and accountable for confirming resolution and closure where required. Acts as the business interface for governance and reporting, typically an IT Manager function.

Service Desk – Consolidated RACI Matrix

Process / Activity	MSP L1	MSP L2	MSP L3	Client Resolver	Vendor	Cross-Service Provider	CAB	Client Service Owner
Incident – Log & Categorise	R, A	-	-	-	-	-	-	I
Incident – Initial Diagnosis & Resolution	R, A	-	-	-	-	-	-	I
Incident – Escalation	R, A	R	R	R (if in-scope)	R (if in-scope)	-	-	I
Incident – Resolution & Recovery	R	R	R	R	R	-	-	I
Incident – Closure Confirmation	R, A	-	-	-	-	-	-	A
Request – Receive & Log	R, A	-	-	-	-	-	-	I
Request – Validate Authorisation	R, A	-	-	-	-	I	-	I
Request – Fulfilment	R, A	R	R (if complex)	R (if in-scope)	-	-	-	I
Request – Confirm Completion	R, A	-	-	-	-	-	-	A
Problem – Detect & Log	R	R	-	-	-	-	-	I
Problem – Root Cause Analysis	-	R	R, A	R (if in-scope)	R	-	-	I
Problem – Workaround Definition	R	R	R, A	-	-	-	-	I
Problem – Permanent Fix	-	R	R, A	R (if in-scope)	R	-	-	I
Problem – Closure	-	R	R, A	-	-	-	-	I
Change – Raise RFC	-	R	R	R	-	-	-	I
Change – Impact Assessment	-	R	R, A	R (if in-scope)	-	-	-	I
Change – Authorisation	-	-	-	-	-	-	A	R
Change – Implementation	-	R	R, A	R (if in-scope)	-	-	-	I
Change – Review & Closure	-	R	R, A	-	-	-	-	I

Pricing & Billing

Flexible billing options are available, as outlined below:

- Minimum quarterly in advance
- Six Monthly in advance
- Annual in advance
- Consumption based, billed in arrears

Each sub-service definition will provide its own commercial packaging (ticket-based, FTE, or hybrid) in alignment with this framework.

Terms & Conditions

The service is governed by Managed 247's Terms and Conditions, available at:

- **Link**: http://managed.co.uk/General-Terms-Conditions.pdf

Appendix A - Service Option Comparison

The following table summarises the inclusions, operating model, and key differentiators across some of the available Service Desk options. Each option is underpinned by the standards and processes set out in the Common Service Definition.

Feature / Scope	Shared Service Desk	Dedicated Service Desk	Co-Managed Service Desk	Out-of-Hours (OOH) Service Desk
Resourcing Model	Multi-tenant resource pool shared across clients	Dedicated resource(s) for a single client	Split responsibilities between MSP and client IT teams	Shared or dedicated coverage outside of standard business hours
Service Coverage	Standard coverage tiers (Business, Extended, 24x7, etc.)	Configurable coverage to client needs (e.g., 8x5 or 24x7 dedicated)	Coverage aligned to split between MSP and client	Covers evenings, weekends, and public holidays as contracted
Escalation Handling	Managed 247 handles all L1 incidents; escalations follow tier model	Full control of incident handling; escalations via agreed runbooks	MSP handles defined tiers; client retains control of others	Focused on urgent incident triage and escalation during OOH
Knowledge & Runbooks	Shared knowledge base leveraged across all clients	Client-specific knowledge base and runbooks maintained	Knowledge base shared between MSP and client teams	Knowledge base leveraged for OOH critical incident handling
Client Experience	Cost-effective, rapid enablement	Bespoke service aligned to client operations	Flexible partnership model	Assurance of round-the-clock coverage
Commercial Model	Ticket-based consumption (baseline + flex)	Ticket-based or	Ticket split or hybrid model (ticket allocation per party)	Ticket-based, typically priced as an add-on
Best Suited For	Clients seeking cost-efficiency with standardised delivery	Clients with high volumes or complex needs requiring dedicated focus	Clients wanting to retain some in-house capability but extend MSP coverage	Clients requiring continuity outside business hours